Created in July 1999, the Office of Independent Oversight and Performance Assurance (OA) provides independent oversight in four areas:

- ***Safeguards and security***
- ***Cyber security***
- ***Emergency management***
- ***Environment, safety, and health***

OA is organizationally independent of Department of Energy (DOE) offices that develop and implement policy and programs. Reporting directly to the Secretary of Energy, OA has no vested interest in the functions it evaluates, and therefore can impartially assess DOE operations.

Office of Cyber Security and Special Reviews (OA-20)

One of five subordinate offices in OA, OA-20's mission is to *independently* assess the effectiveness of DOE cyber security policy and program implementation.

Role of the OA-20 Laboratory

The Cyber Security Laboratory provides the tools for objectively assessing DOE cyber security performance. It provides the capability to determine whether the various technical and managerial components of cyber security are integrated for effective protection of critical, sensitive electronic information.

OA subject matter experts attempt penetrations of DOE computer networks by using techniques similar to those a hacker or sophisticated attacker might use to penetrate any computer system. The techniques include:

- Remotely scanning DOE site networks from the Internet for a realistic view of a site's potential vulnerability to external threats
- Penetration testing to determine the potential magnitude and associated risk posed by vulnerabilities identified during scanning
- Evaluating new vulnerabilities and "exploits" for penetrating computer networks
- Assessing protection and vulnerabilities of internal DOE computer networks to malicious insider activities, using portable computers and tools.

OA-20 Assures Protection of Sensitive Information

DOE's mission is diverse, encompassing national security, environmental quality, national power distribution, and energy and scientific research. OA's role is to review the different kinds of computer networks supporting these functions in order to assess how well DOE is protecting critical infrastructure assets and the security of its classified and sensitive unclassified information. The different kinds of computer networks include:

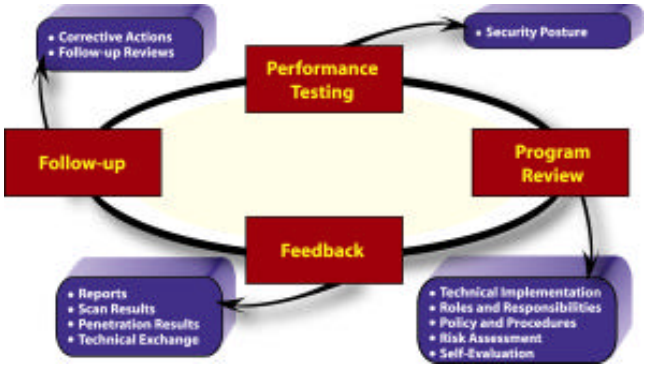
- Internal computer networks that support a variety of functions that contain sensitive unclassified information
- Classified information networks, linked to other types of networks, that support activities associated with nuclear weapons stockpile stewardship
- Publicly accessible networks that provide information on DOE activities.

The OA Cyber Security Laboratory performs different types of assessments to evaluate whether the configuration of these network systems minimizes Department-wide risk and exposure to cyber attacks:

- External Network Security Assessments – Simulating a hacker from the Internet by scanning and conducting penetration testing from a remote location; may be announced or unannounced ("Red Team")
- Internal Network Security Assessments – Simulating an attack from a malicious insider by scanning and conducting penetration testing from within the DOE network
- Review of Trust Relationships – Analyzing whether certain connections are potentially exploitable by reviewing connections between DOE sites and offsite organizations, such as satellite offices, support contractors, universities, and governmental organizations
- Testing Need-to-Know Boundaries – Ensuring that internal users have access only to the information that they need to know to accomplish their job, by conducting tests of logical boundaries and reviewing network configurations
- Assessing Intrusion Detection Capabilities – Ensuring that sufficient measures are in place to detect intruders at all levels of the network, by conducting tabletop reviews and assessing response to penetration tests.

Laboratory Activities Are Integrated with Management Reviews

Performance testing may identify weaknesses resulting from implementation or management issues. Management reviews focus on processes that are necessary to improve and sustain an effective cyber security program. Most OA-20 assessments use a combination of performance testing and management reviews, resulting in a comprehensive assessment of the key areas of a cyber security program, as shown below.



OA-20 Laboratory Challenge

Now more than ever, the only constant in the cyber workplace is change. OA's Cyber Security Laboratory provides for the systematic evaluation of the Department's cyber security and provides essential feedback for planning continuous improvement in DOE's cyber security strategies and policies. The Lab meets the challenge of keeping pace with emerging technological advances and new exploits, a necessity for protecting sensitive information.

For further information, please visit our web site at **http://www.oa.doe.gov** or call (301) 903-3777.

October 2002